Daily Open Source Infrastructure Report
08 October 2015

Top Stories

- Cincinnati-based Fifth Third Bank will pay $85 million October 6 to settle civil fraud allegations that they improperly certified 1,439 defective Federal Housing Administration mortgage loans, resulting in millions of dollars of losses. – *Cincinnati Enquirer* (See item **4**)
- The U.S. Centers for Disease Control and Prevention reported October 5 an Oklahoma resident was the fourth death tied to a 35-State Salmonella outbreak, increasing the total number of illness to 732 people. – *Associated Press* (See item **11**)
- Researchers from Cisco shut down a massive ransomware campaign accounting for 50 percent of all ransomware deployments via the Angler exploit kit (EK) that would have allowed the campaign's operators to collect over $34 million. – *Softpedia* (See item **19**)
- The South Carolina Emergency Management Division reported that at least 11 dams have failed in the State while another 35 are being monitored October 7 due to heavy storms that led to 17 deaths, water outages for tens of thousands, road closures, and building evacuations. – *CNN* (See item **25**)

Fast Jump Menu

PRODUCTION INDUSTRIES
- Energy
- Chemical
- Nuclear Reactors, Materials, and Waste
- Critical Manufacturing
- Defense Industrial Base
- Dams

SUSTENANCE and HEALTH
- Food and Agriculture
- Water and Wastewater Systems
- Healthcare and Public Health

SERVICE INDUSTRIES
- Financial Services
- Transportation Systems
- Information Technology
- Communications
- Commercial Facilities

FEDERAL and STATE
- Government Facilities
- Emergency Services

Energy Sector

1. *October 6, New Hampshire Union Leader* – (New Hampshire) **Generator explosion and fire shut down Bethlehem biomass energy plant.** The Pinetree Power facility in Bethlehem, New Hampshire, was shut down indefinitely October 6 following a generator explosion and fire. The incident remains under investigation.
   Source: http://www.unionleader.com/Generator-explosion-and-fire-shut-down-Bethlehem-biomass-energy-plant

2. *October 6, Washington Observer-Reporter* – (Pennsylvania) **DEP approves First Energy's plan to ship coal ash to Hatfield's Ferry landfill.** The Pennsylvania Department of Environmental Protection approved a permit modification the week of September 21 which allows First Energy to use the coal ash landfill at the closed Hatfield's Ferry Power Plant in Greene County to dispose of coal ash and scrubber waste from the landfill at its Bruce Mansfield Power Plant in Shippingport.
   Source: http://www.observer-reporter.com/article/20151006/NEWS02/151009629

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

Nothing to report

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

3. *October 6, WTVR 6 Richmond* – (Virginia) **Sheriff: Three men arrested in cigarette, illegal credit card bust in Caroline County.** Caroline County authorities arrested a New Yorker and two Jamaican citizens October 6 after finding over 100 fraudulent credit cards, electronics, and skimming devices in their vehicle in Caramel Church, Virginia.
   Source: http://wtvr.com/2015/10/06/sheriff-three-men-arrested-in-cigarette-illegal-credit-card-bust-in-caroline-county/

4. *October 6, Cincinnati Enquirer* – (National) **Fifth Third pays $85M to settle mortgage fraud.** Federal officials announced October 6 that Cincinnati-based Fifth Third Bank will pay $85 million to settle civil fraud allegations that the company knowingly improperly certified 1,439 defective Federal Housing Administration

mortgage loans, resulting in millions of dollars of losses to the agency from 2003 – 2013.
Source: http://www.usatoday.com/story/money/nation-now/2015/10/06/fifth-third-pays-85m-settle-mortgage-fraud/73492444/

5. *October 6, WBRZ 2 Baton Rouge* – (National) **Third arrest made in BR-based national financial fraud scheme.** Louisiana officials announced October 6 the arrest of the third suspect in a national financial fraud scheme in which conspirators allegedly stole over 300 identities and committed over $5 million in fraud. The suspect reportedly provided bogus credit repair services for free and helped issue stolen Social Security numbers and used the numbers for fraudulent loan applications.
Source: http://www.wbrz.com/news/third-arrest-made-in-br-based-national-financial-fraud-scheme/

Transportation Systems Sector

6. *October 7, Delaware County Daily Times* – (Pennsylvania) **Conchester Highway finally reopens after being shut down for hours by overnight crash.** A portion of U.S. Route 322 from Baltimore Pike to Interstate 95 in Pennsylvania was shut down overnight October 6 due to an accident that took down power lines and a pole. No injuries were reported.
Source: http://www.delcotimes.com/general-news/20151006/conchester-highway-finally-reopens-after-being-shut-down-for-hours-by-overnight-crash

7. *October 6, USA Today* – (New Mexico) **United flight diverts after pilot becomes ill, loses consciousness.** A United Airlines flight headed to San Francisco from Houston diverted to Albuquerque, New Mexico, October 6 after one of the pilots became ill and passed out. The plane landed safely and the pilot was taken to a hospital.
Source: http://www.usatoday.com/story/todayinthesky/2015/10/06/reports-united-flight-diverts-after-pilot-becomes-ill-loses-consciousness/73462082/

8. *October 6, KABB 29 San Antonio* – (Texas) **One person killed in three car crash in Kendall County.** A stretch of Highway 46 in Kendall County was shut down for approximately 3 hours October 6 while crews responded to a 3-vehicle accident that killed 1 person.
Source: http://www.foxsanantonio.com/news/features/top-stories/stories/one-person-killed-three-car-crash-kendall-county-16425.shtml#.VhUUpPlVhBc

For another story, see item **25**

Food and Agriculture Sector

9. *October 6, U.S. Food and Drug Administration* – (National) **General Mills voluntarily recalls a limited quantity of frozen Cascadian Farm Cut Green Beans.** Minneapolis-based General Mills issued a voluntary class 2 recall October 2 of its limited quantity of frozen Cascadian Farm Cut Green Beans packaged in 16-ounce bags after 1 package of finished product tested positive for Listeria monocytogenes. The

product was distributed to retail establishments nationwide.
Source: http://www.fda.gov/Safety/Recalls/ucm465921.htm

10. *October 6, U.S. Food and Drug Administration* – (Colorado; California) **Snack Out Loud Foods issues allergy alert on undeclared milk in Snacks Out Loud Sea Salt Crunchy Bean Snacks 1.2oz single serve units.** Snack Out Loud Foods recalled 56 cases of its Sea Salt Crunchy Bean Snacks October 6 due to misbranding after subsequent investigation revealed a temporary breakdown in the company's production and packaging processes which did not list milk as an ingredient. The product was distributed to retail stores in Colorado and California.
Source: http://www.fda.gov/Safety/Recalls/ucm465989.htm

11. *October 6, Associated Press* – (Oklahoma) **1 dead in Oklahoma from multistate salmonella outbreak.** The U.S. Centers for Disease Control and Prevention reported that an Oklahoma resident was the fourth death tied to a 35-State Salmonella outbreak, increasing the total number of illness to 732 people after each person consumed tainted cucumbers gown in Mexico.
Source: http://www.kjrh.com/news/state/1-dead-in-oklahoma-from-multistate-salmonella-outbreak

Water and Wastewater Systems Sector

12. *October 6, Albany Times Union* – (New York) **East Greenbush officials address health crisis at flood-damaged sewer plant.** East Greenbush officials ordered emergency repairs to the municipal sewer plant October 6 after heavy rains September 29 – 30 overwhelmed the plant and caused extensive damage to the facility that is undergoing a $13 million rebuilding project. The flood water caused an overflow of the treatment tanks and carved away the new concrete foundation.
Source: http://www.timesunion.com/business/article/East-Greenbush-sewers-hit-again-with-state-6553042.php

13. *October 6, KFSM 5 Fort Smith* – (Arkansas) **City of Hartford under boil order following main water line break.** Officials issued a boil order October 6 for the city of Hartford in Arkansas after a water main line ruptured while crews were putting in a new water line. Authorities stated that the order will remain active for at least a week while water samples are tested.
Source: http://5newsonline.com/2015/10/06/city-of-hartford-under-boil-order-following-main-water-line-break/

14. *October 6, Reuters* – (Michigan) **Michigan providing water filters in Flint after high lead readings.** Free water filters were distributed to residents of Flint, Michigan, October 6 after the State confirmed a study the week of September 28 by Hurley Children's Hospital that determined children had increased levels of lead in their blood due to city's drinking water.
Source: http://www.reuters.com/article/2015/10/06/usa-michigan-flint-idUSL1N1262MI20151006

For another story, see item **25**

Healthcare and Public Health Sector

15. *October 7, WFLA 8 Tampa* – (Florida) **Watch: $100,000+ worth of drugs stolen from St. Pete Walgreens.** Police are searching for a suspect who stole over $100,000 worth of prescription painkillers from a Walgreens in St. Petersburg October 5 by forcing open the pharmacy counter's locked shutter.
Source: http://wfla.com/2015/10/06/watch-suspect-takes-more-than-100000-worth-of-drugs-from-walgreens/

Government Facilities Sector

Nothing to report

Emergency Services Sector

16. *October 6, Associated Press* – (Nevada) **Kingman prison riot update: 11 inmates indicted in July 1 riot.** Eleven inmates were charged for their involvement in a July 1 riot at the Cerbat Unit at a private prison in Kingman, Arizona, that began when an officer tried to stop an inmate-on-inmate attack. The incident spurred follow-up riots July 2 and July 4, and led to nine corrections officers suffering injuries and approximately $1.9 million in damages to the prison.
Source: http://www.abc15.com/news/region-northern-az/other/kingman-prison-riot-update-11-inmates-indicted-in-july-1-riot

Information Technology Sector

17. *October 7, Securityweek* – (International) **Malicious Android adware infects devices in 20 countries.** Security researchers from FireEye were monitoring a new malicious adware campaign dubbed Kemoge that has affected Android devices in 20 countries, in which the malware serves ads to an infected device, extracts exploits to root phones, and employs multiple persistence mechanisms. The malware is packaged with popular Android apps uploaded to third-party stores.
Source: http://www.securityweek.com/malicious-android-adware-infects-devices-20-countries

18. *October 7, Softpedia* – (International) **Zero-day exploit found in Avast antivirus.** Security researchers from Google's Project Zero discovered a zero-day exploit in Avast antivirus software in which an attacker could leverage a faulty method used for parsing X.509 certificates in secure connections to execute code on an affected system. Avast has since patched the vulnerability.
Source: http://news.softpedia.com/news/zero-day-exploit-found-in-avast-antivirus-493958.shtml

19. *October 7, Softpedia* – (International) **Major ransomware campaign disrupted, attackers lose potential revenues of $34M.** Researchers from Cisco shut down a

massive ransomware campaign accounting for 50 percent of all ransomware deployments via the Angler exploit kit (EK) that would have allowed the campaign's operators to collect over $34 million. The cyber-criminals used a network of 147 proxy servers bought from Limestone Networks via stolen credit cards to deliver the largest ransomware delivery platform ever noticed in the wild.
Source: http://news.softpedia.com/news/major-ransomware-campaign-disrupted-attackers-lose-potential-revenues-of-34m-493924.shtml

20. *October 7, Help Net Security* – (International) **Previously unknown Moker RAT is the latest APT threat.** Security researchers from enSilo discovered a new Remote Access Trojan (RAT) dubbed Moker that takes over targeted systems by creating a new user account before opening a RDP channel to gain remote control, and tampers with sensitive system and security files and settings. The malware comes with a complete feature set and, achieves system privileges, and may also be controlled locally.
Source: http://www.net-security.org/malware_news.php?id=3124

21. *October 7, The Register* – (International) **Remote code exec hijack hole found in Huawei 4G USB modems.** Security researchers from Positive Technologies discovered cross-site scripting (XSS) and stack overflow vulnerabilities in Huawei E3272 USB 4G modem that could allow attackers to conduct remote execution and denial-of-service (DoS) attacks and hijack connected computers. Huawei released patches addressing the vulnerabilities.
Source:
http://www.theregister.co.uk/2015/10/07/remote_code_exec_hijack_hole_found_in_huawei_4g_usb_modems/

22. *October 6, Securityweek* – (International) **Winnti spies use bootkit for persistence, distributing backdoors.** Security researchers from Kaspersky Lab discovered that the advanced persistent threat (APT) group Winnti has been using an attack platform dubbed "HDRoot" as a bootkit disguised to look like Microsoft's Net.exe utility while protected by VMProtect software, delivering two backdoors. The group previously targeted gaming companies in the U.S. and worldwide.
Source: http://www.securityweek.com/winnti-spies-use-bootkit-persistence-distributing-backdoors

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: http://www.us-cert.gov

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: http://www.it-isac.org

Communications Sector

Nothing to report

Commercial Facilities Sector

23. *October 7, WLS 7 Chicago* – (Illinois) **Fire tears through Shrine of Christ the King in Woodland.** Dozens of people were evacuated from Shine of Christ the King Church in Chicago October 7 after a 3-alarm fire began on the second floor and spread to the roof of the building. More than 150 firefighters were on the scene extinguishing the flames and officials reportedly believe the fire began from varnishing work completed overnight October 6.
Source: http://abc7chicago.com/news/woodlawn-church-fire-under-control/1020949/

24. *October 7, KABC 7 Los Angeles* – (California) **3-alarm fire damages 10 buildings in Florence.** A 3-alarm fire in Florence heavily damaged 10 buildings housing 12 businesses, displaced 6 people, and prompted up to 250 firefighters to extinguish the blaze October 7. No injuries were reported and the cause of the fire remains under investigation.
Source: http://abc7.com/news/3-alarm-fire-damages-12-businesses-in-florence/1020980/

For another story, see item **25**

Dams Sector

25. *October 7, CNN* – (South Carolina) **South Carolina flooding: Dams breached, more trouble.** The South Carolina Emergency Management Division reported that at least 11 dams have failed in the State while another 35 are being monitored October 7 due to heavy rain storms that have led to 17 deaths, water outages for tens of thousands, road closures, and building evacuations.
Source: http://foxct.com/2015/10/07/south-carolina-flooding-dams-breached-more-trouble-ahead/

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: http://www.dhs.gov/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer